Fraud and irregularity

Annual report 2022/23

AUDIT SCOTLAND

Contents

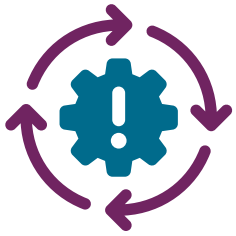
Accessibility

You can find out more and read this report using assistive technology on our website.

For information on our accessibility principles, please visit: www.audit-scotland.gov.uk/accessibility.

Key messages

1 During 2022/23, 12 cases of fraud and irregularity valued over £139,000 were identified. Weaknesses in internal controls contributed to each case identified.



2 Auditors have found that public bodies have effective systems, procedures and controls in place to help prevent and detect the majority of fraud and irregularity.

Recommendations

Public bodies should ensure they have effective counter-fraud arrangements. This includes:

- undertaking a fraud risk assessment to identify areas at risk
- having effective counter-fraud governance arrangements
- having a counter-fraud strategy and regularly reviewing counter-fraud plans
- regular assessment and review of internal controls
- considering the control weaknesses identified in this report.

Auditors should review:

- whether counter-fraud governance arrangements are effective and regularly reviewed and revised as necessary
- the effectiveness of counter-fraud controls along with the details on the control weaknesses identified in this report.

Fraud and irregularity identified during 2022/23

Auditors provide Audit Scotland with details of fraud and irregularity discovered in their audited bodies. This report sets out the cases identified during 2022/23 including the details of the control weaknesses which contributed to these cases.

Aims of this report

1. This report shares information where control weaknesses have contributed to fraud and irregularity. This report aims to help prevent similar situations happening in other bodies by sharing the details and highlighting weaknesses in internal controls. Other cases of fraud or irregularity may exist that were not facilitated by weaknesses in internal controls. External auditors[1] identified 12 cases of fraud and irregularity totalling over £139,000 in audited bodies in 2022/23 (seven cases totalling £401,500 were identified in 2021/22). This level of fraud and irregularity is very small when compared to the £56.5 billion Scottish budget.[2]

2. The cases included in this report have been investigated internally but will not necessarily have been reported to Police Scotland or to have been proven as fraud in a court of law.

3. This report encourages public bodies to consider the cases included in this report and reflect whether the same control weaknesses exist in their own systems. Public bodies are also encouraged to regularly review their counter-fraud arrangements to ensure they remain effective against both existing and newly emerging types of fraud and irregularity.

4. The case studies in this report aim to help auditors consider and review the effectiveness of the counter-fraud governance arrangements in their audited bodies.

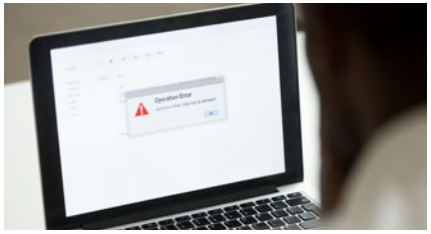
1 External auditors report frauds, or suspected frauds, to Audit Scotland where they are caused or facilitated by weaknesses in public bodies' internal controls. Frauds and irregularities are considered significant where the value of the loss is over £5,000 or where it is of significance owing to the nature of the activity.

2 Scottish Budget 2022 to 2023: Your Scotland, Your Finances – guide

Fraud and irregularity cases identified in 2022/23

Fraud and irregularity identified during 2022/23 totalled over £139,000 and fell into the following categories:

5 cases
Grant payments



1 case
Invalid supplier

1 case
Procurement card

1 case
School funds

3 cases
Payroll and pensions

1 case
Theft

Control weaknesses

The following control weaknesses contributed to the fraudulent and irregular activity identified during 2022/23.

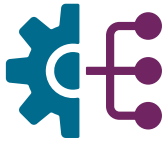
Not checking all details on applications for funding

Lack of management checking

No independent confirmation with the customer before changing bank account details

Not following procedures

A lack of segregation of duties



Weak authorisation processes

Lack of awareness of potential fraud risks

Poor security arrangements

Specific details of the fraud and irregularity cases identified during 2022/23 are on the following pages.

Expenditure

Expenditure fraud relates to cases where a body has incurred additional expenditure because of fraud. This may be due to invalid suppliers, fictitious invoicing, or the redirection of payments intended for legitimate suppliers.

Case study 1.
Grant payments

Four unknown third parties made four fraudulent grant applications for Covid-19 support totalling £51,000.

Key features

Supporting documentation and proof of bank account evidence was provided. The frauds were possible as there were small differences in the business name and email address which were not picked up. The bank accounts used to facilitate the fraud were included in a suspicious activity report; however, due to pressure to ensure grants were paid without delay the applications were processed and paid despite this.

In one case, the fraud was identified after the grant payment was rejected by the bank. In the other cases, a retrospective data-matching exercise identified the frauds.

Retrospective checking including use of a national data-sharing facility has since been carried out on all Covid-19 grant payments.

Case study 2.
Grant payments

An unknown individual compromised a grant recipient's email account and committed bank mandate fraud. A grant of £12,300 was subsequently paid to the fraudulent bank account.

Key features

After informing the grant applicant that their application was successful, the council received a request to change the grant recipient's bank account details.

The request came from the genuine grant recipient's email account and contained an attachment on headed paper requesting the change. The bank details were then changed.

The fraud was identified when the genuine grant recipient reported non-receipt of the funds.

The fraud could have been prevented if the council had contacted the grant recipient to confirm the bank account changes.

The council have since issued bank mandate guidance for staff and existing controls have been strengthened.

Case study 3.
Invalid supplier

A third party defrauded over £11,000 from a public body by purporting to be a supplier to the body.

Key features

The public body received a request by email to amend a supplier's bank account details. The supplier's email address had been intercepted by a fraudster who requested the change.

The fraud was possible as the public body did not telephone the supplier to verify the change of bank details.

The issue was identified when the genuine supplier queried why the payment had not been received.

The public body's counter-fraud team has reviewed the process for changing suppliers' bank account details and improvements have been made to procedures.

The matter has been reported to Police Scotland.

Case study 4.
Procurement card

A manager misused a procurement card to the extent of £5,450 to withdraw cash fraudulently and to make fraudulent payments.

Key features

The fraud was identified when the manager was on leave and another member of staff looked for the cash.

The fraud was possible as management did not check procurement card receipts or supporting documentation prior to approving expenditure.

The body is reviewing the number of procurement cards holders and approvers and staff are required to complete refresher training on procurement cards. The manager has been dismissed.

Case study 5.
School funds

A head teacher embezzled over £5,300 from a school fund.

Key features

The teacher fraudulently used the school fund purchase card, which was held in the name of another member of staff, for personal purchases. The teacher also falsified an invoice to disguise the payment of a personal membership fee, and misappropriated school fund concert cash that had been entrusted to the teacher.

The fraud was identified after concerns were raised regarding misappropriation of the school fund purchase card.

Subsequent investigations identified that high-value items purchased from the school fund could not be located on the school premises. These items were subsequently recovered from the teacher's home.

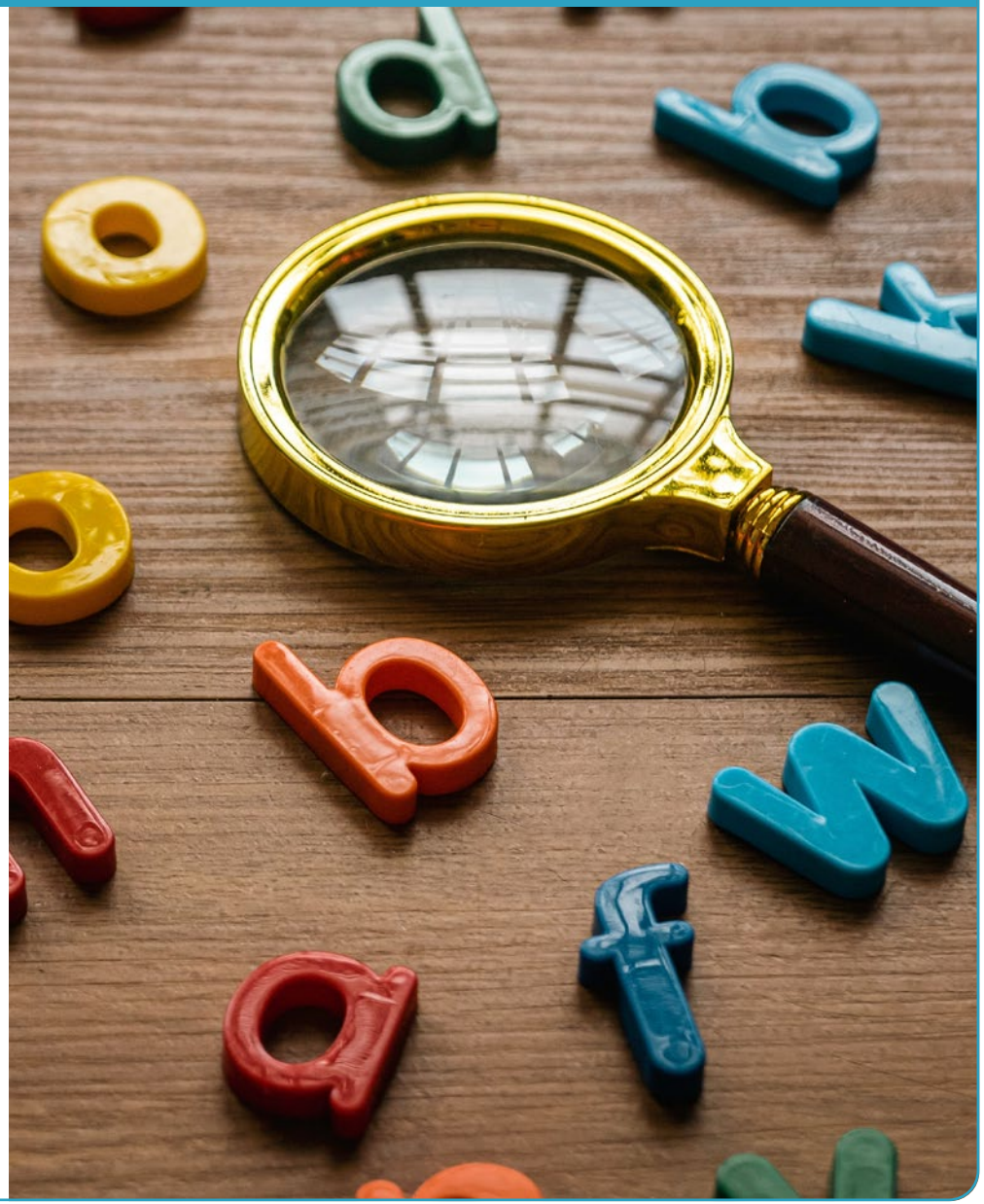
The fraud was possible as, due to the seniority of the teacher; the actions were not challenged by other staff. In practice, there was no segregation of duties.

The council has:

- revised school fund procedures
- introduced random sampling of purchase card transactions
- provided fraud awareness and procurement training to school staff.

The case has been reported to the Procurator Fiscal. The teacher resigned following the instigation of disciplinary proceedings.

Items to the value of £1,600 have been recovered.



Payroll and pension fraud

Payroll and pension fraud relates to people receiving payroll or pension payments to which they are not entitled.

Case study 6.
Payroll fraud

A council employee failed to report a £25,000 payroll overpayment over a three-year period.

Key features

An error in processing a reduction in working hours resulted in an increase to the employee's salary. The error was not identified by the authorising officer, and the employee did not report the overpayment.

The fraud was identified during a data check carried out by the council. The fraud was not detected earlier as the normal annual data checks were suspended during the pandemic.

The council has issued reminder instructions to staff processing and authorising payroll amendments to emphasise the importance of ensuring that details are correct. A new checking process has been introduced that requires staff to verify any change of working hours requests to amendment forms, contracts, and payroll details.

Disciplinary action has been taken and recovery action is in process.

Case study 7.
Payroll fraud

An ex-council employee failed to report a £10,500 payroll overpayment over a seven-month period.

Key features

The employee left the council's employment and moved to a health board following a secondment period. However, the council salary continued to be paid for seven months after the employee left the council.

The fraud was identified when the health board queried an invoice for recovery of the employee's costs.

The fraud was possible as the employee's manager in the council failed to complete a termination form.

The manager has been reminded of the requirement to complete termination forms. The council has reintroduced a previously suspended monthly report requiring managers to confirm the employment status of employees in their service.

A repayment plan is in place to recover the overpayment.

Case study 8.
Pension payments

A third party claimed over £6,600 from a widower's pension following his death.

Key features

The fraudster had notified the pension fund of a change of bank details for receipt of the pension after the pensioner had died. This notification came from the same email account used for the original bank mandate. The personal details provided, along with the signature, matched those on the original bank mandate and it was processed.

The fraud was identified as part of the National Fraud Initiative (NFI).

The fraud was possible as there was limited consideration given to the potential risks associated with the receipt of new bank details. An internal audit investigation identified recommendations to help strengthen controls around changes to bank details.

Police Scotland identified the individual who submitted the fraudulent bank mandate and, following a police caution, the full amount was repaid.

Theft

Theft relates to cases where someone acts dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it.

Case study 9.
Theft

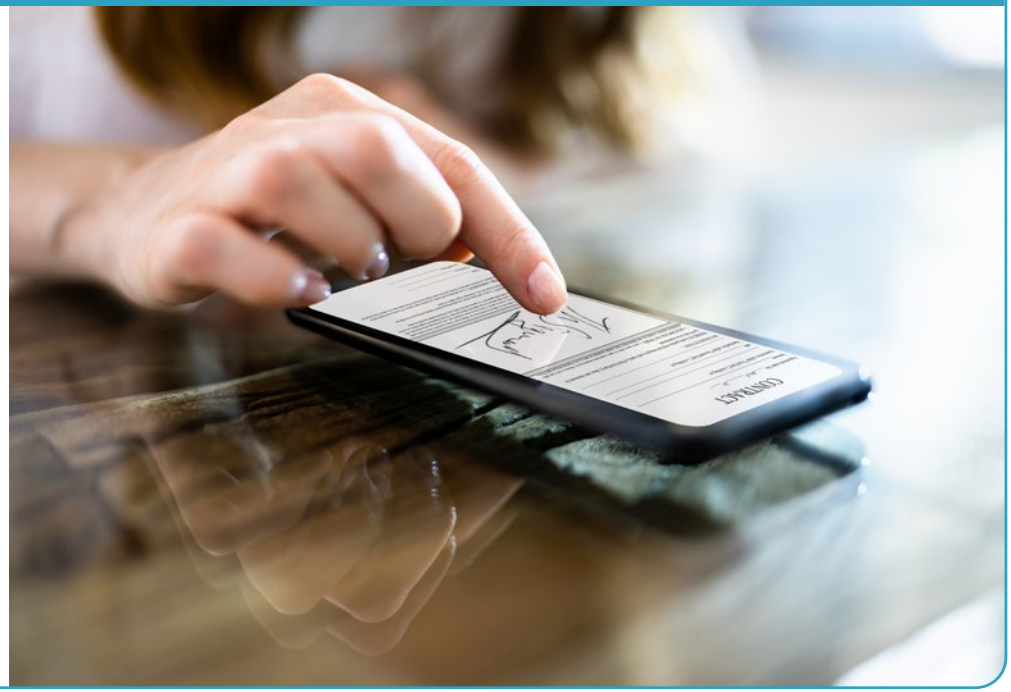
An unidentified perpetrator stole random access memories (RAMs) valued at £12,000 from laptops stored in the office of a public body.

Key features

It was discovered during a stock check that some laptops had been opened and RAMs removed.

The theft was possible due to poor security arrangements. The perpetrator has not been identified due to the absence of CCTV.

Security procedures have been strengthened and a process for controlling the distribution of laptops has been developed.



Further information

Further information about Audit Scotland's work on counter-fraud is available on our website. This includes information on:

Our counter-fraud work

The National Fraud Initiative

Red flags in procurement

Cybercrime: A serious risk to Scotland's public sector

SEPA continues to count cost of cyber-attack

Fraud and irregularity

Annual report 2022/23

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
Phone: 0131 625 1500 Email: **info@audit-scotland.gov.uk**
www.audit-scotland.gov.uk

ISBN 978 1 915839 18 3